kaspersky

Jak vzdělávat své zaměstnance na kybernetickou bezpečnost

Petr Kuboš | Enterprise Sales Manager CZ a SK

Fakta o Kaspersky

> 22
let historie

> 4,000
vysoce kvalifikovaných zaměstnanců

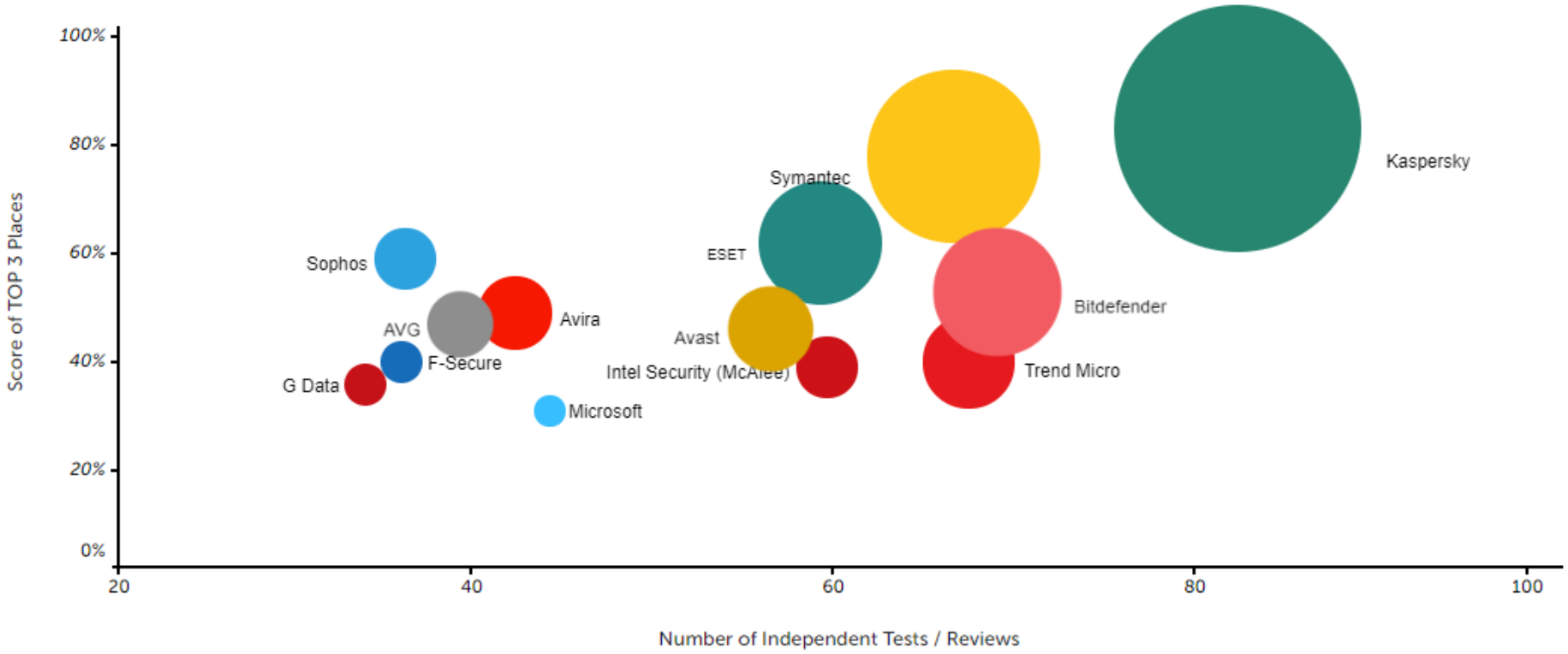
> 400,000,000
uživatelů celosvětově je chráněno našimi technologiemi

> 270,000
firemních zákazníků celosvětově

> Celosvětově největší, soukromě vlastněná bezpečnostní společnost

Kaspersky ochrana – nejvíce testována, nejlépe oceňována.

V roce 2019 se produkty Kaspersky Lab zúčastnily 86 nezávislých testů a recenzí. V 64 případech obsadily první místo a v 81% skončily v první trojce.



MOST TESTED*
MOST AWARDED*
KASPERSKY LAB
PROTECTION

*Notes:

- According to summary results of independent tests in 2019 for corporate, consumer and mobile products.
- Summary includes independent tests conducted by: AV-Comparatives, AV-Test, SE Labs, MRG-Effitas, Virus Bulletin, ICSA Labs, PCSL, NSS Labs.
- Tests performed in these programs assess all protection technologies against known, unknown and advanced threats.
- The size of the bubble reflects the number of 1st places achieved.

https://www.kaspersky.com/top3

kaspersky

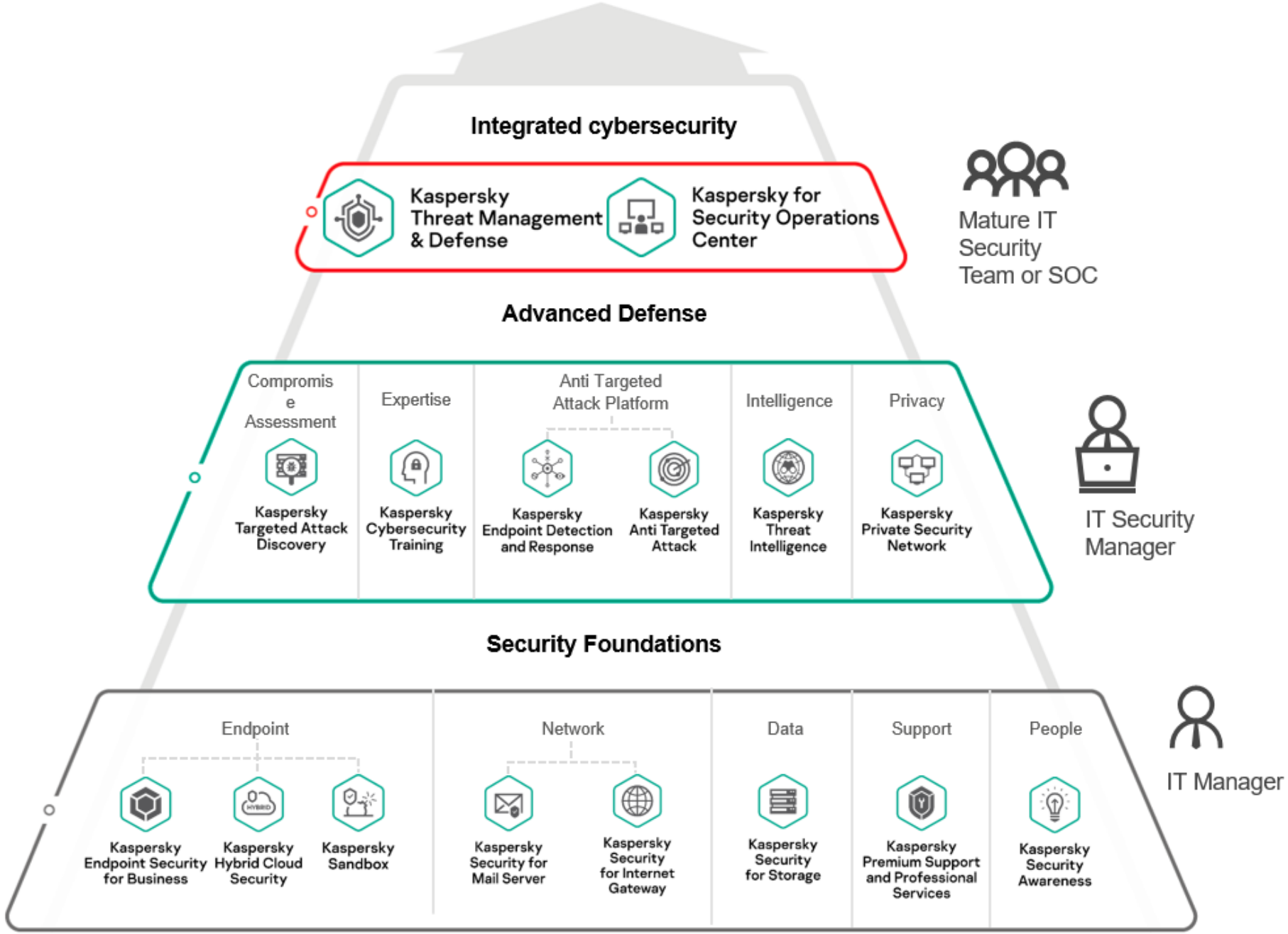
Transparency – a new cybersecurity trend

Globálně propojený svět vyžaduje zvýšenou transparentnost. Společnost Kaspersky pokračuje ve vývoji své „Global Transparency Initiative“ , jejímž cílem je prokázat náš trvalý závazek zajistit integritu a důvěryhodnost řešení společnosti ve službách našich zákazníků.

Data storage and processing	Ve švýcarských datových centrech jsme začali uchovávat veškerá data Evropských zákazníků a zpracovávat škodlivé a podezřelé soubory které s námi Kaspersky zákazníci sdílejí.
Transparentní centra	Otevřeli jsme transparency centra v Curychu, Švýcarsku a Madridu, Španělsku a v Kuala Lumpur. Čtvrté středisko transparentnosti v Brazílii bude otevřeno v průběhu roku 2020
Bug bounty program	Zvýšili jsme odměny za nalezení chyb v produktech Kaspersky až na 100 000 $ za objevenou zranitelnost

„ Komise nedisponuje žádnými důkazy týkající se potenciálních problémů souvisejících s používáním produktů společnosti Kaspersky Lab. “

EU Commissioner for Digital Economy and Society


Integrated cybersecurity
Kaspersky Threat Management & Defense
Kaspersky for Security Operations Center
Mature IT Security Team or SOC
Advanced Defense
Compromise Assessment
Kaspersky Targeted Attack Discovery
Expertise
Kaspersky Cybersecurity Training
Anti Targeted Attack Platform
Kaspersky Endpoint Detection and Response
Kaspersky Anti Targeted Attack
Intelligence
Kaspersky Threat Intelligence
Privacy
Kaspersky Private Security Network
IT Security Manager
Security Foundations
Endpoint
Kaspersky Endpoint Security for Business
Kaspersky Hybrid Cloud Security
Kaspersky Sandbox
Network
Kaspersky Security for Mail Server
Kaspersky Security for Internet Gateway
Data
Kaspersky Security for Storage
Support
Kaspersky Premium Support and Professional Services
People
Kaspersky Security Awareness
IT Manager

kaspersky

Vývoj malwaru

kaspersky

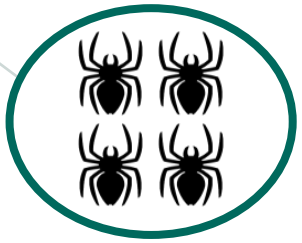
STUPNICE NÁRUSTU HROZEB

1994

1
NOVÝ VIRUS
KAŽDOU
HODINU

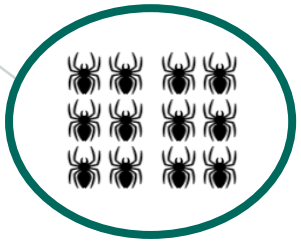
2006

1
NOVÝ VIRUS
KAŽDOU
MINUTU



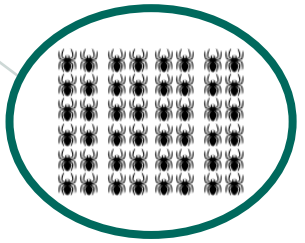
2011

1
NOVÝ VIRUS
KAŽDOU
SEKUNDU



2014 - 2019

+300,000
NOVÝCH
VZORKŮ
KAŽDÝ DEN



kaspersky

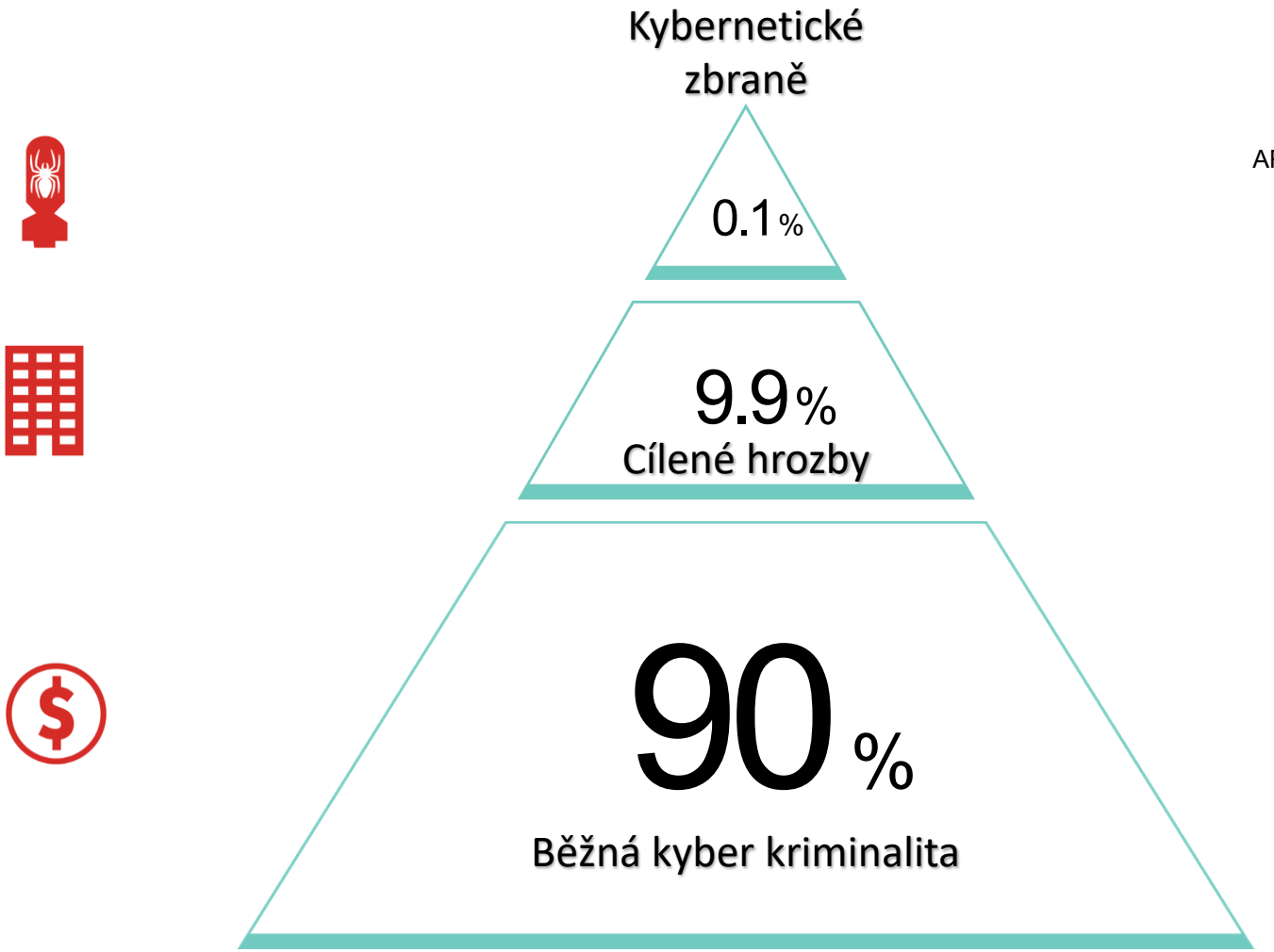
+360,000

Kaspersky detekuje více než 360,000 nových unikátních

škodlivých vzorků, denně.

kaspersky

Skladba kybernetických hrozeb



APT – pokročilé persistentní hrozby a útoky,

Cílené útoky a pokročilý malware

„běžné“ hrozby

Profi IT Security Team or SOC

IT Security Manager

IT Manager

Kybernetické hrozby

jsou realitou dnešních dnů.

kaspersky

Hlavní rizika obchodních společností v roce 2018

Narušení provozuschopnosti

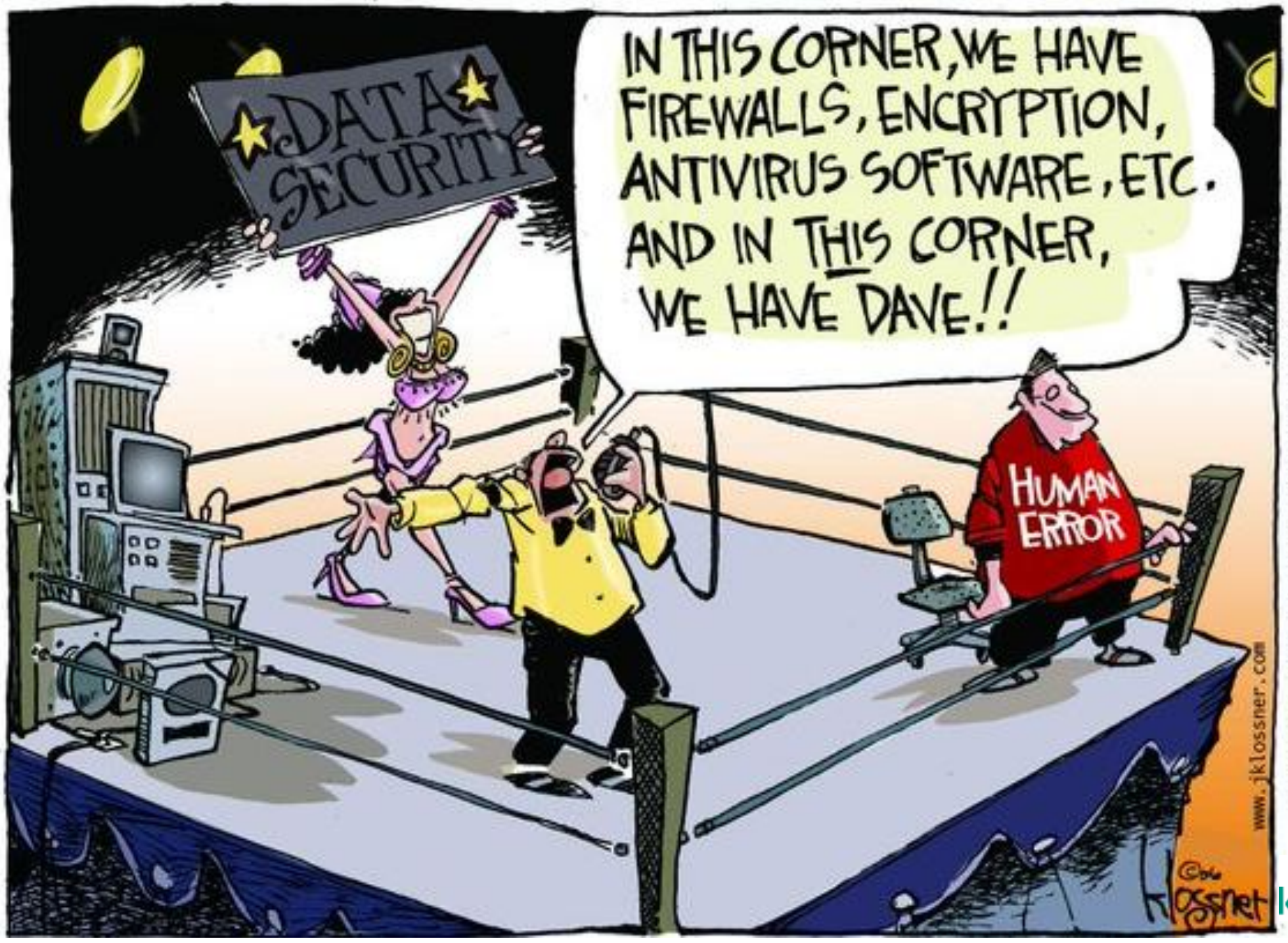
Kybernetické hrozby

2018 - **2**
2017 - 3
2015 - 5
2014 - 8
2013 - 13

2018

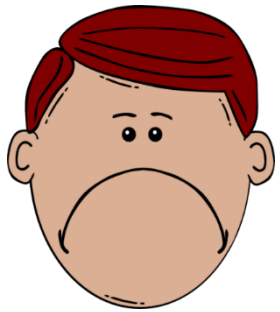
http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2018.pdf

kaspersky



SECURITY TODAY

UŽIVATELÉ JSOU TEN NEJSLABŠÍ ČLÁNEK



Až 80% všech kybernetických incidentů jsou způsobeny lidskými chybami. Společnosti utrácejí miliony za jejich nápravu.

kaspersky

Lidský faktor jako významná bezpečnostní hrozba

Chování zaměstnanců je pro organizace významná IT bezpečnostní hrozba, navzdory tomu, že jsou využívány tradiční způsoby školení zaměstanců.

$1,057,000

v Enterprise organizaci

Průměrný finananční dopad způsobený únikem dat a kybernetickými incidenty zaměstnanců či nedostatečnými IT zdroji

$98,000

v SMB

Průměrný finananční dopad způsobený únikem dat a kybernetickými incidenty zaměstnanců či nedostatečnými IT zdroji

$101,000

v SMB

Finanční dopad útoků způsobených phishingem. *

up to $400

na zaměstnance a rok

Průměrné náklady na řešení phishingového útoku

Kaspersky | Security Awareness

* *Report: "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives . Kaspersky Lab, 2019*

** *Report: "Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within", Kaspersky Lab and B2B International, June 2017.*

** *Calculations based on Ponemon Institute, "Cost of Phishing and Value of Employee Training", August 2015.*

Proč je důležité vybrat si ten správný vzdělávací program?

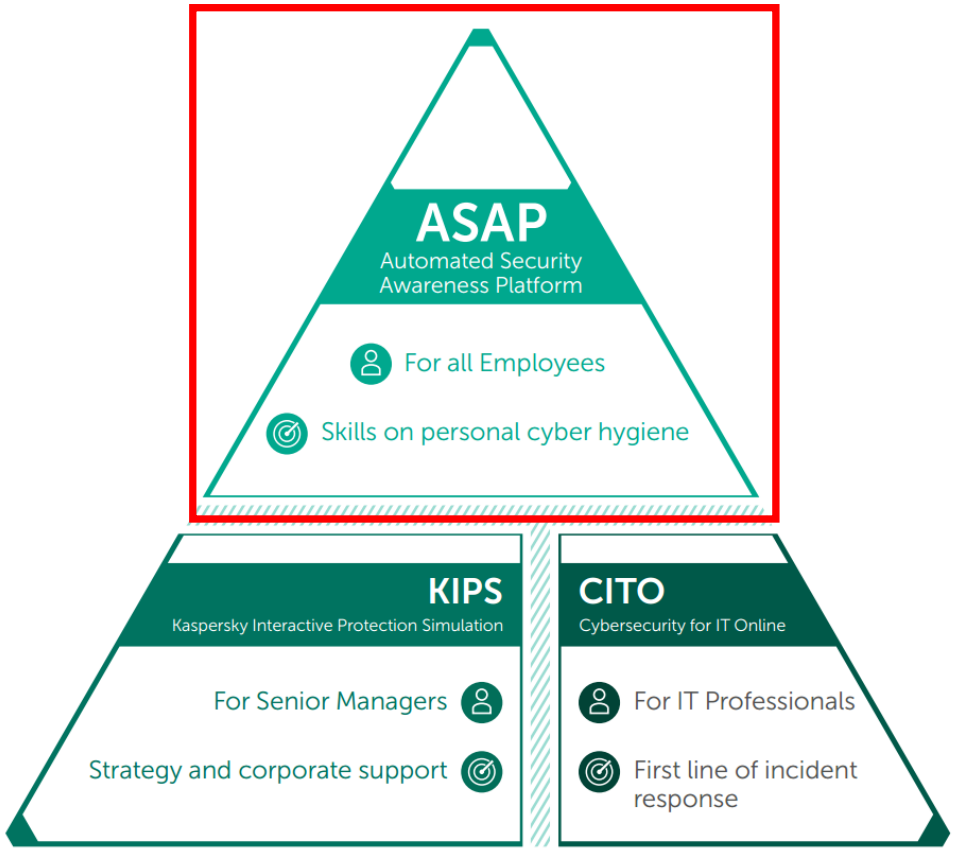
Nezajímavé a neefektivní pro zaměstnance:

- Považován za obtížné, nudné, nedůležité.
- Většinou je to o : „co nesmíte“ než „jak na to“
- Účastníci si po školení nic nepamatují
- Čtení a poslouchní není efektivní

Přítěž pro administrátory:

- Jak vytvořit vzdělávací program a nastavit cíle školení?
- Jak zvládnout proces vzdělávání?
- Jak kontrolovat průběžné výsledky?
- Jak oslovit zaměstance aby se zapojili do školení

Kaspersky
vzdělávací programy kybernetické bezpečnosti



Praktické dovednosti místo jen znalostí

PC orientované, jednoduché na správu a doručení, skvělý reporting.

Příklady z reálného světa & praktické cvičení – zaměstnanci jsou motivováni a zapojeni do vzdělávacího programu

Jednoduchá správa pro administrátory a efektivní pro organizaci

Redukuje počet lidských chyb a selhání až o

80%

kaspersky

kaspersky

TRY NOW CONTACT US ENGLISH

01

02

03

04

05

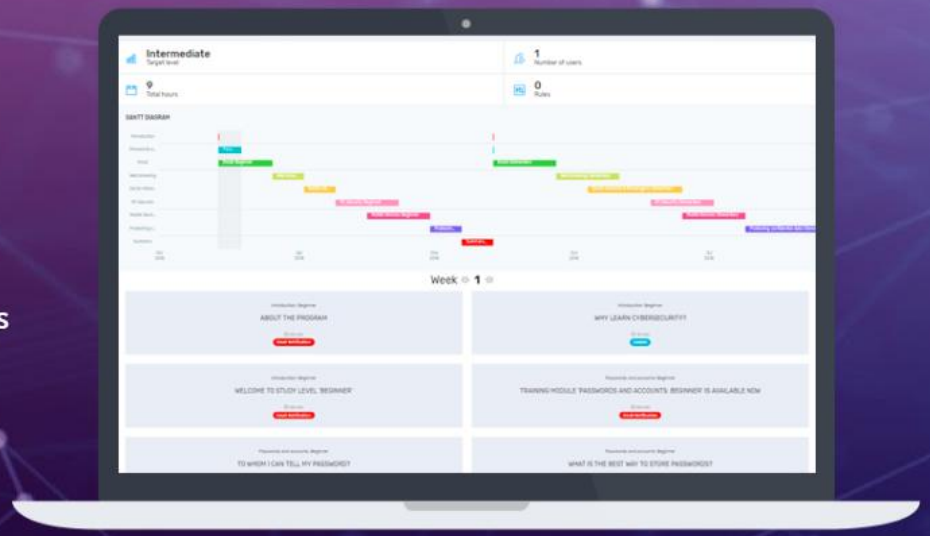
Kaspersky Automated Security Awareness Training

An easy-to-manage online tool which builds employee's cybersecurity skills level by level

Kaspersky Automated Security Awareness Platform (ASAP) is created by leading cybersecurity experts to protect your business

Launch your awareness program online in just a few steps

TRY NOW >



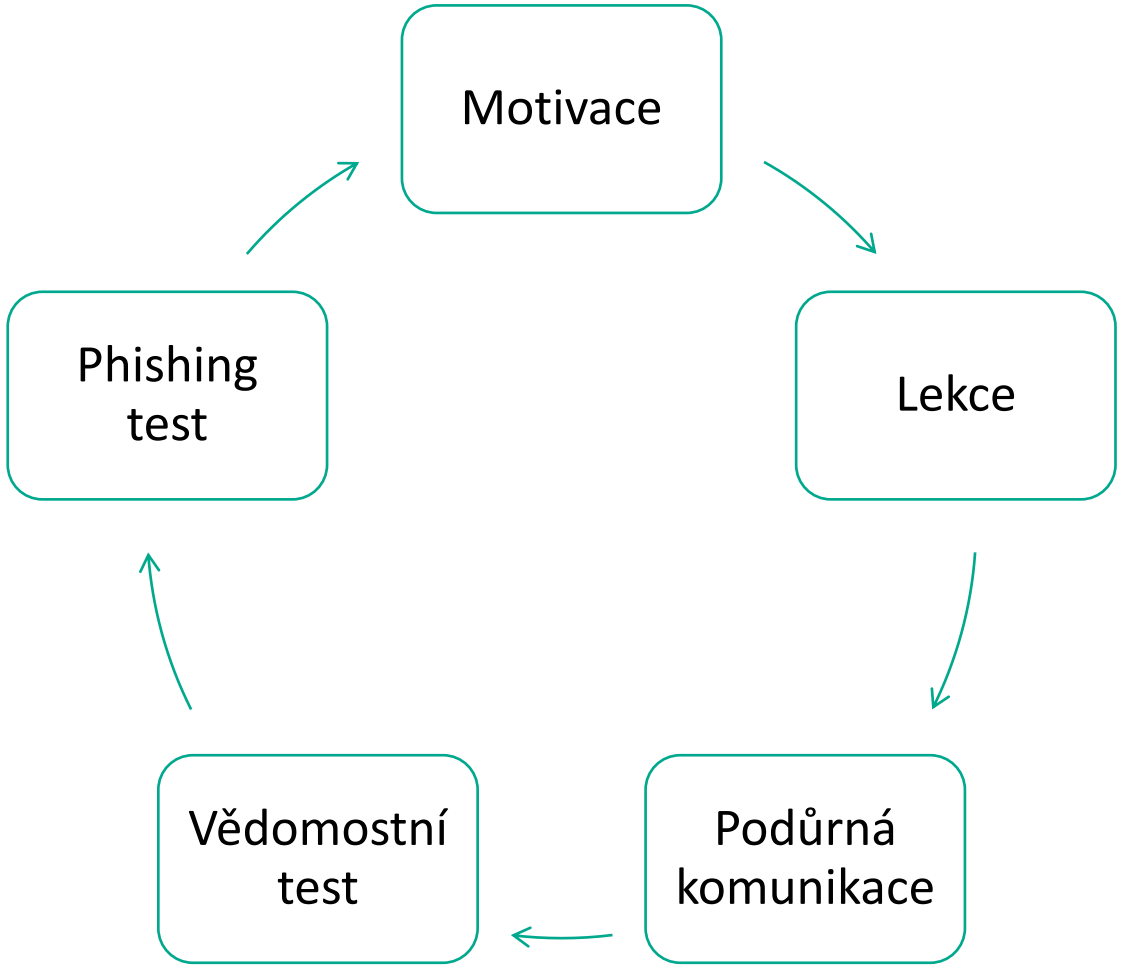
View Datasheet

View Demo

Kaspersky | Security Awareness

Free trial
k-asap.com

Automatizovaná vzdělávací platforma

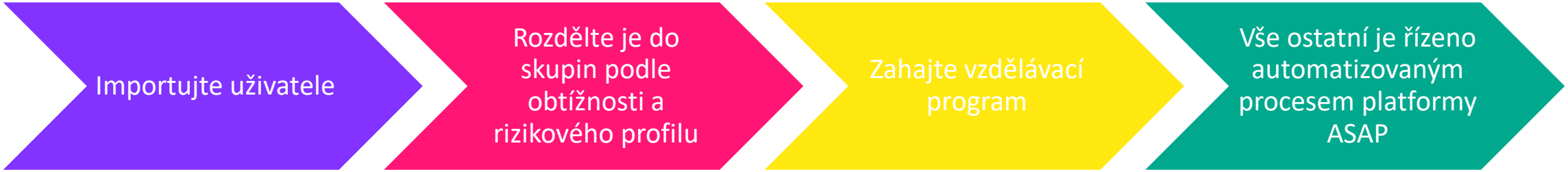


- Všechny typy vzdělávacích modulů jsou automaticky naplánovány a automaticky přiřazeny uživatelům.
- Vzdělávací cyklus se opakuje v průběhu délky licenčních podmínek
- Témata jsou logické a časově nezaťěžují studující uživatele.

kaspersky

Plně automatizovaná podpora a správa vzdělávací platformy

Jak začít vzdělávat své zaměstnance?



Pouze tento krok vyžaduje vaší úvahu a rozhodnutí o rozdělení do profilů

Vše ostatní, jako:

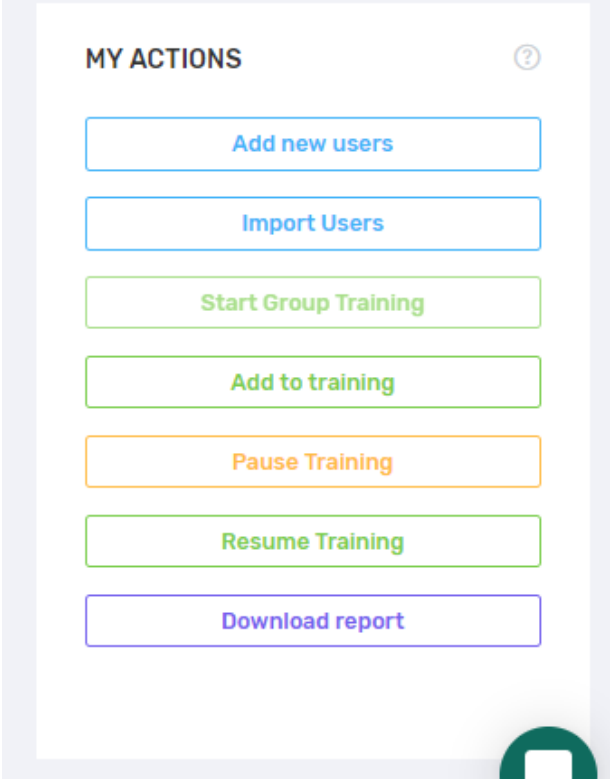
- Individuální plánovaní programu
- Individuální týdenní reporty pro zaměstnance
- Pravidelné reporty pro administrátory

Budou provedeny automaticky bez zásahu administrátora.

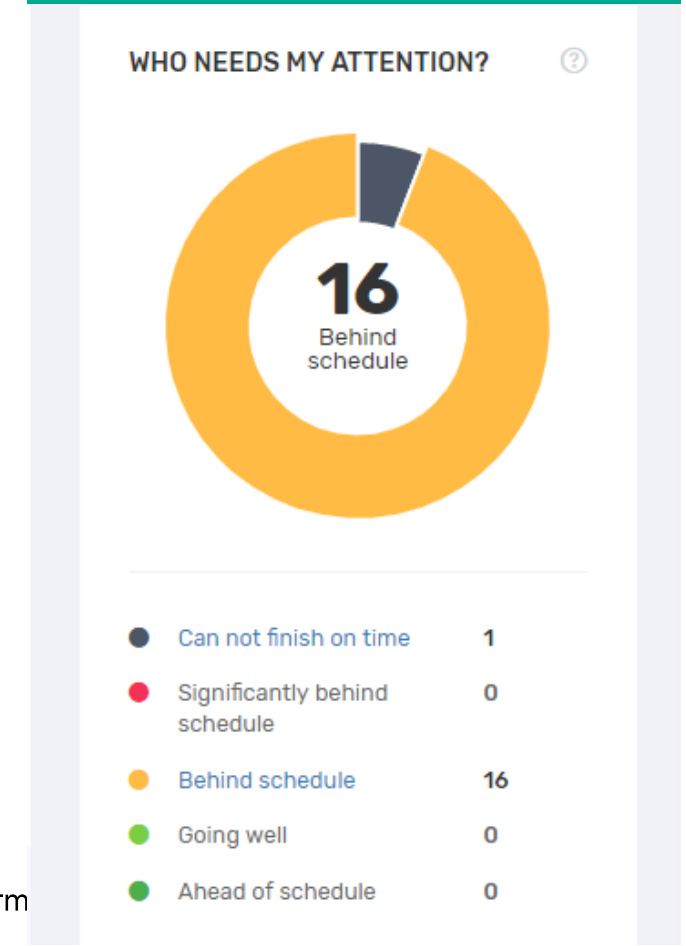
kaspersky

Jednoduchý ovládací panel - vše na jednom místě...

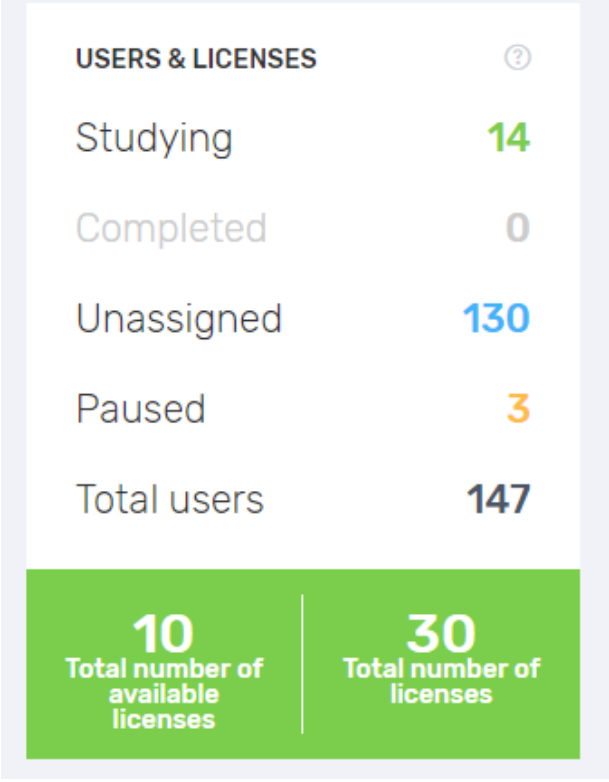
BĚŽNÉ ÚKOLY



STUDENTI POTŘEBUJÍCÍ POMOC

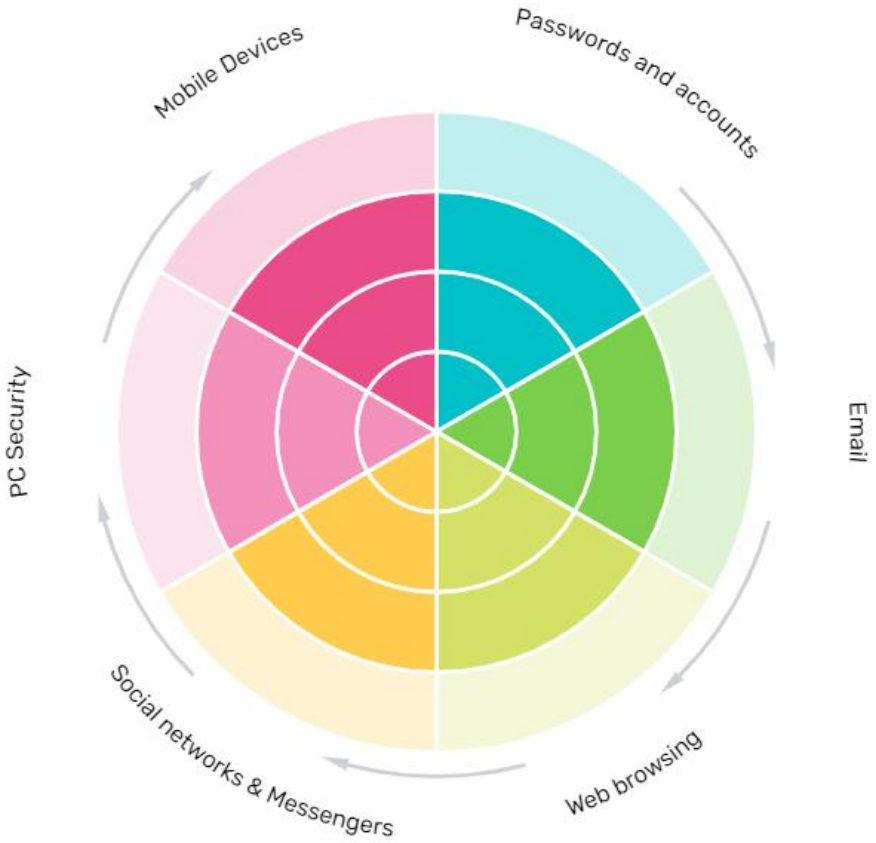


PŘEHLED LICENCÍ



kaspersky

Automatizovaná vzdělávací platforma (ASAP)



Více než 350 lekcí strukturovaných do 3 úrovní obtížnosti a 6 témát

- Hesla a účty
- Email
- Web browsing
- Social networks & messengers
- PC Security
- Mobile devices

+ Různé druhy vzorů phishingových emailů

Dostupné v 10 jazycích

CZ a SK verze – červen 2020

Free trial: k-asap.com

kaspersky

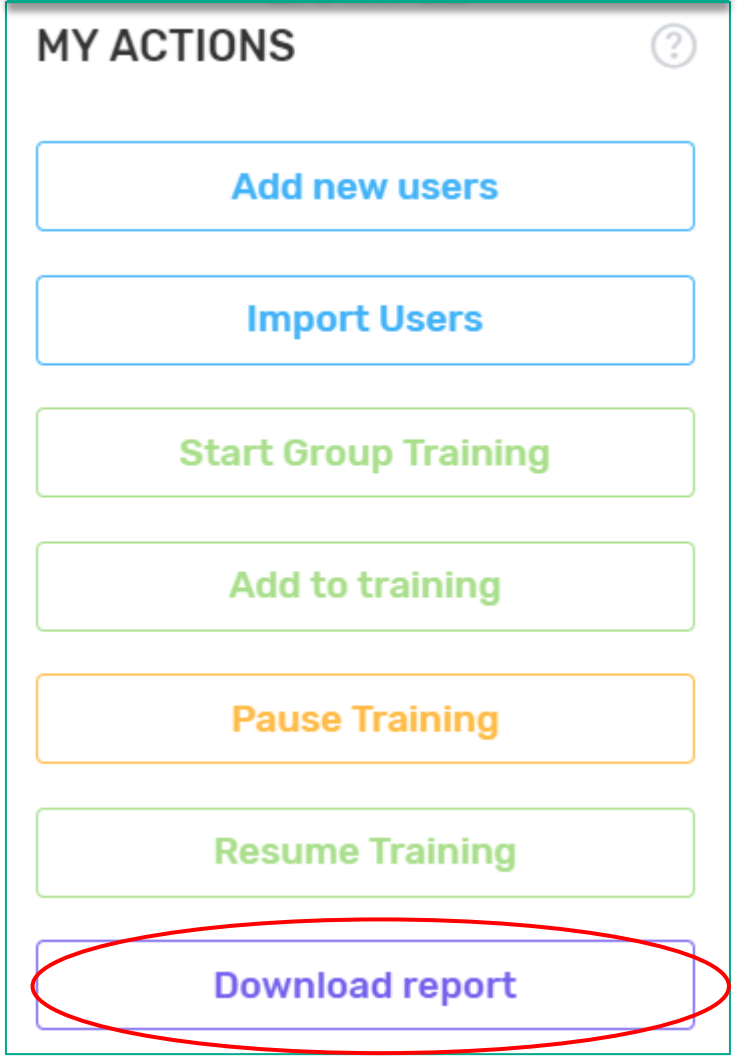
Report pouze 1 klinutím

Report si můžete stáhnout pouze 1 kliknutím.

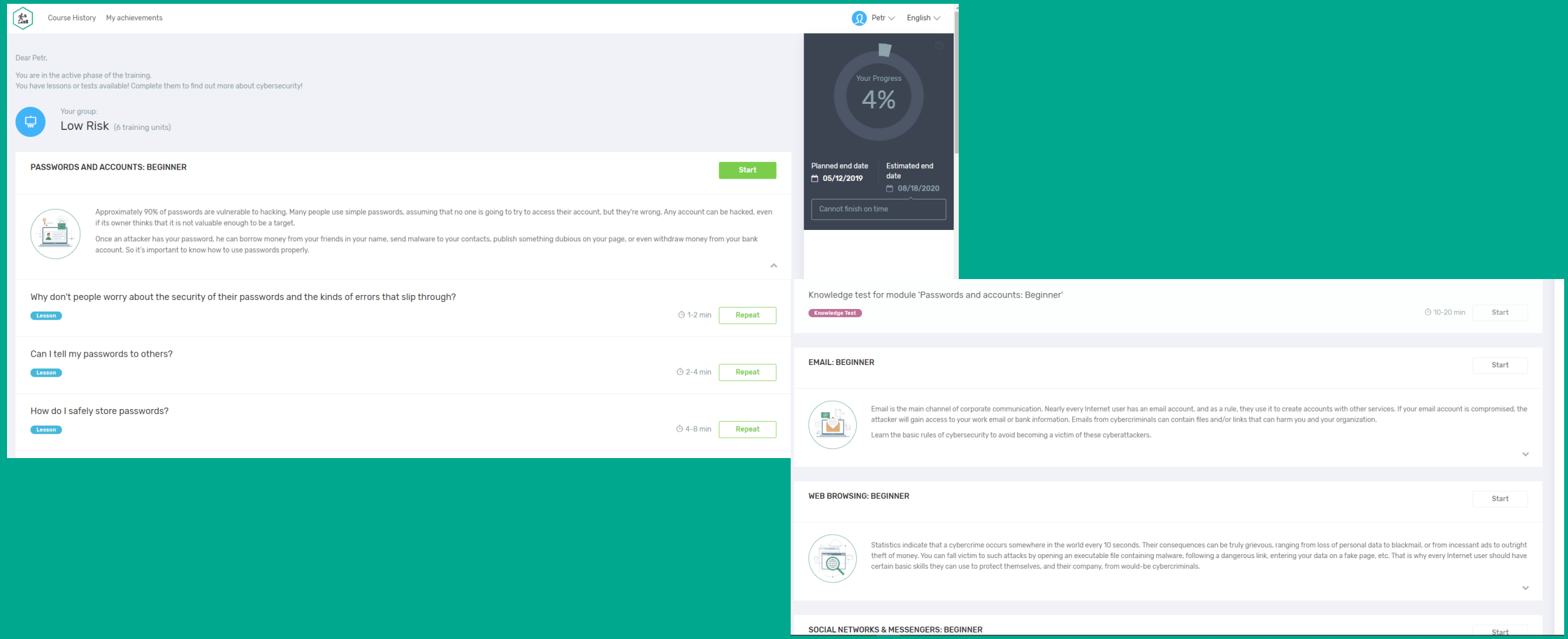
USERS' PERFORMANCE REPORT EXAMPLE

Total users	1500		
Study status for each one:			
Unassigned	17		
Studying	1483		
Paused	0		
Completed	0		
Archived	0		
Licenses in Use	1483		
Who needs my attention?			
Study Speed	Number of Users	Reasons For Falling Behind	Number of Users
Total Studying	1483		
Ahead of schedule	31		
Going well	1386		
Behind schedule	58	Do not take tests	3
		Fail tests	55
		Never entered the platform	0
Significantly behind schedule	8	Do not take tests	6
		Fail tests	2
		Never entered the platform	0
Can not finish on time	0	Do not take tests	0
		Fail tests	0

PLATFORM INTERFACE EXAMPLE



Uživatelské rozhraní - náhled



ASAP obchodní model

- License začínající od 5 uživatelů
- Cena za 1 rok / 1 uživatel, podle celkového počtu uživatelů
- Spravujte více společností pod jedním účtem
- Online web verze – v případě SCORM offline verze
- Zkouška na období 2 měsíců pro 3 uživatele, zdarma
- Demo interaktivního modulu

kaspersky

TRY NOW CONTACT US ENGLISH

01

02

03

04

05

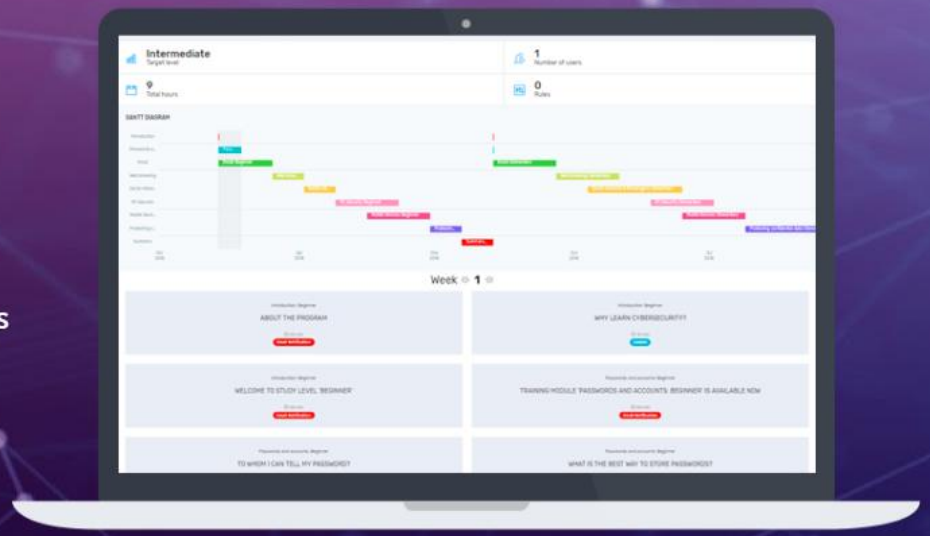
Kaspersky Automated Security Awareness Training

An easy-to-manage online tool which builds employee's cybersecurity skills level by level

Kaspersky Automated Security Awareness Platform (ASAP) is created by leading cybersecurity experts to protect your business

Launch your awareness program online in just a few steps

TRY NOW >



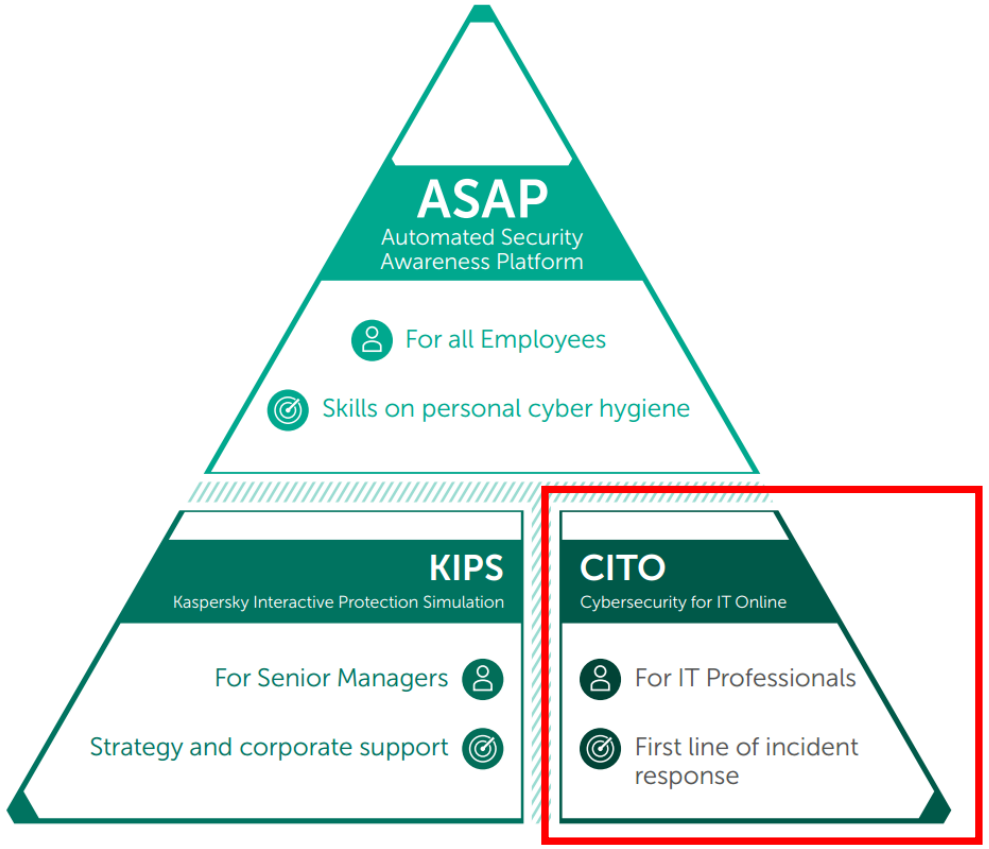
View Datasheet

View Demo

Kaspersky | Security Awareness

Free trial
k-asap.com

Kaspersky Security Awareness - CITO



Cyber Seurity for IT Online

Efektivní školení pro všechny IT specialisty

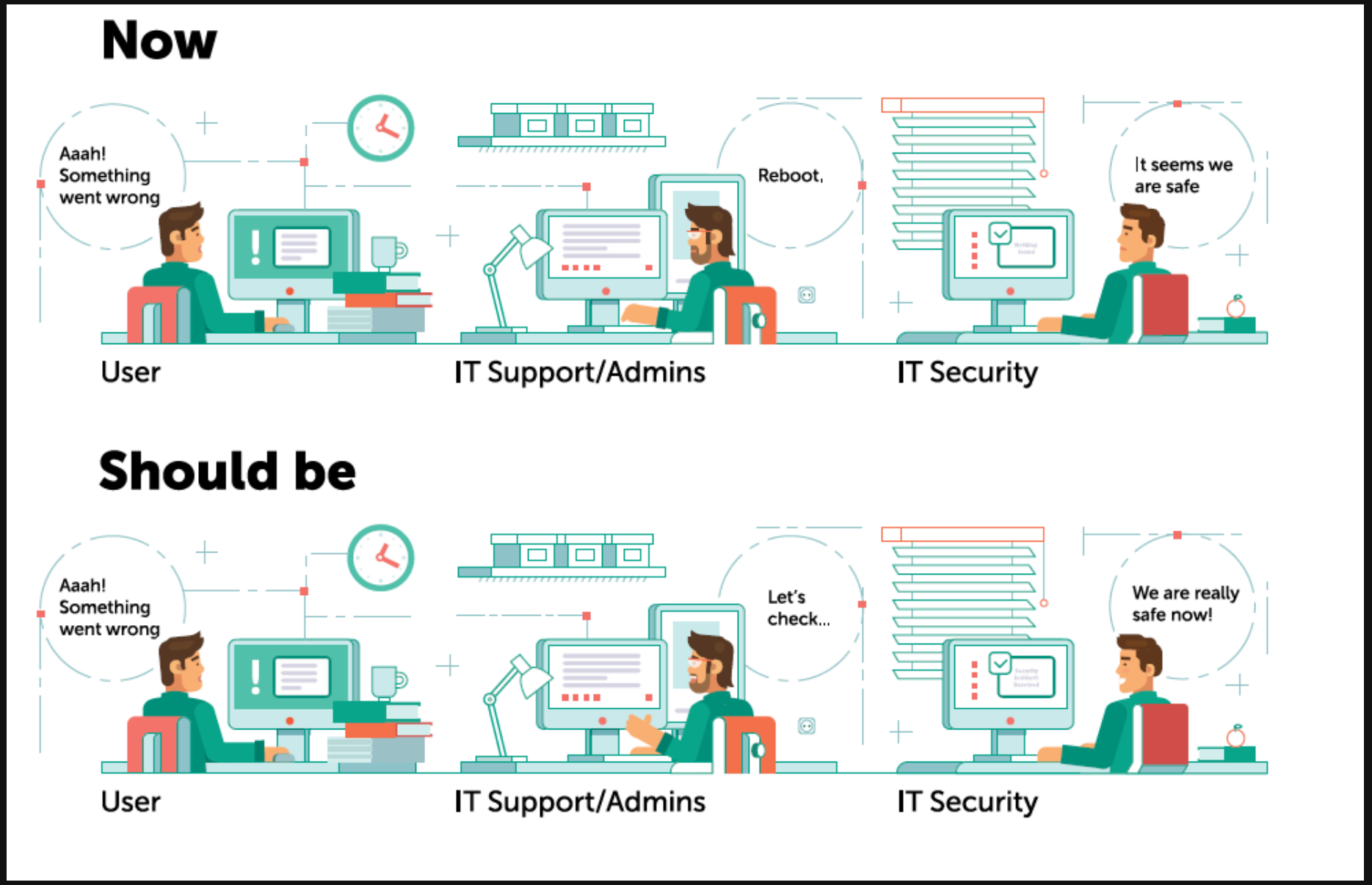
https://cito.cloudapp.net/

Snižuje počet lidských chyb až o:

80%

kaspersky

IT specialisté – Nové role a odpovědnosti – dříve a nyní



KASPERSKY lab

Cybersecurity For IT Online

Cíle vzdělávání ?

- Kritické myšlení o bezpečnosti v IT
- Znalost hackerských nástrojů a technik
- Základní dovednosti analýzy hrozeb
- Znalosti, jak pomoci bezpečnostnímu oddělení při reakci na incident

Pro koho je určeno ?

- Service desky
- IT / síťoví profesionálové
- IT bezpečnost
- Místní správci a další technicky pokročilí zaměstnanci

4 moduly, ~ 30 praktických cvičení

Malicious Software

Verification of existence or absence of incident related to malware

#Processhacker, #Autoruns, #Fiddler, #GMER

Potential unwanted Programs

Working with event monitors of the systems and sandboxes. Using statistical engines (virustotal). Removing PuPs

#ProcessMonitor, #Cuckoo, #Virustotal

Phishing Incident Response

Phishing emails lookup. Verification of the incident related to phishing. OSINT

#ExchangeComplianceSearch , #Robtex, #Whois, #GoogleDorks

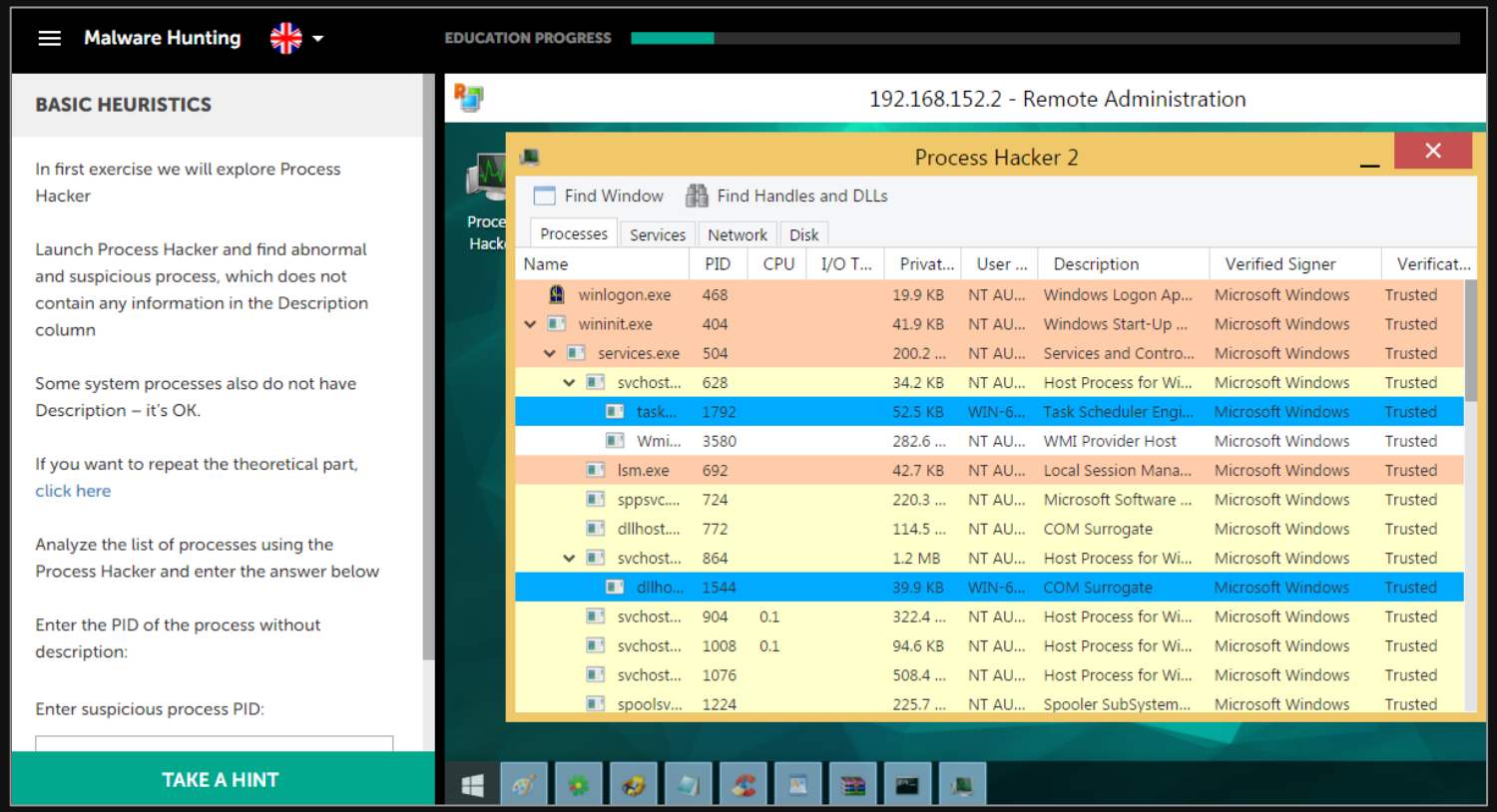
Investigation Basics

Incident localization, data collection, collecting digital evidence, log and timeline analysis

#EventLogExplorer, #Autopsy, #FTK-Imager

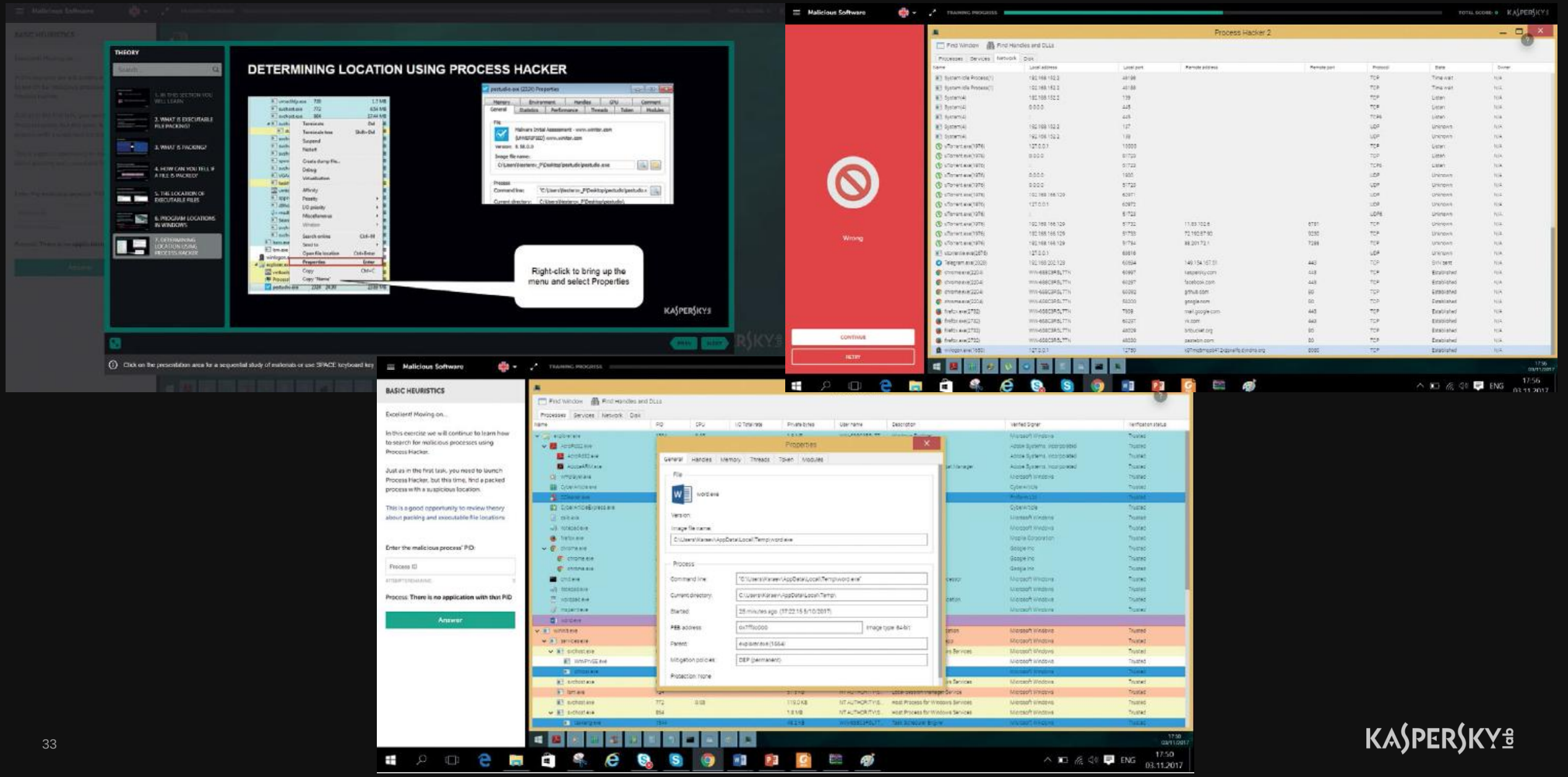
Cybersecurity For IT Online

Awareness => incident response training



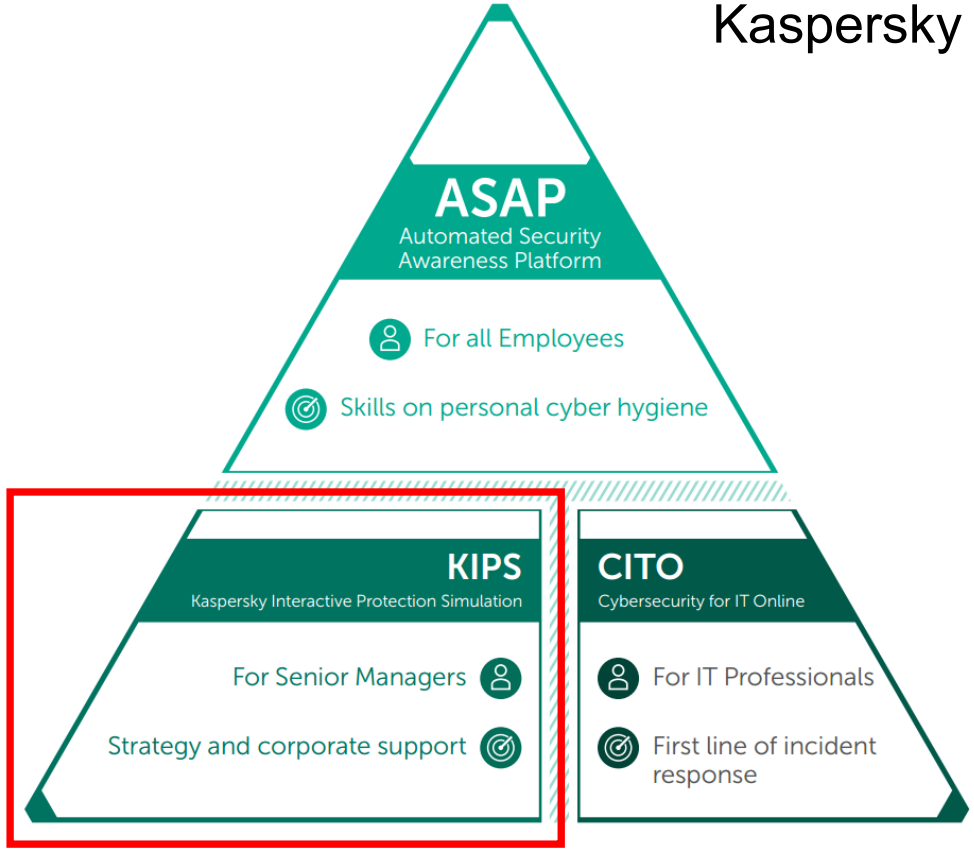
Cíle školení:

- Posílit „první linii obrany“ v reakci na kybernetické incidenty
- Snížit počet incidentů způsobených chybnou konfigurací
- Rozvíjet kritické myšlení týmů IT o kybernetické bezpečnosti



KASPERSKY lab

Kaspersky Security Awareness - KIPS



Kaspersky Interactive Protection Simulation

Snižuje
počet lidských chyb až o:

80%

kaspersky

Cybersecurity today – lost in a ‘corporate bermuda triangle’

CEO

Does not see how cybersecurity spendings relate to Revenues

SECURITY

Focus on protecting the confidential information

Many security controls are under IT management

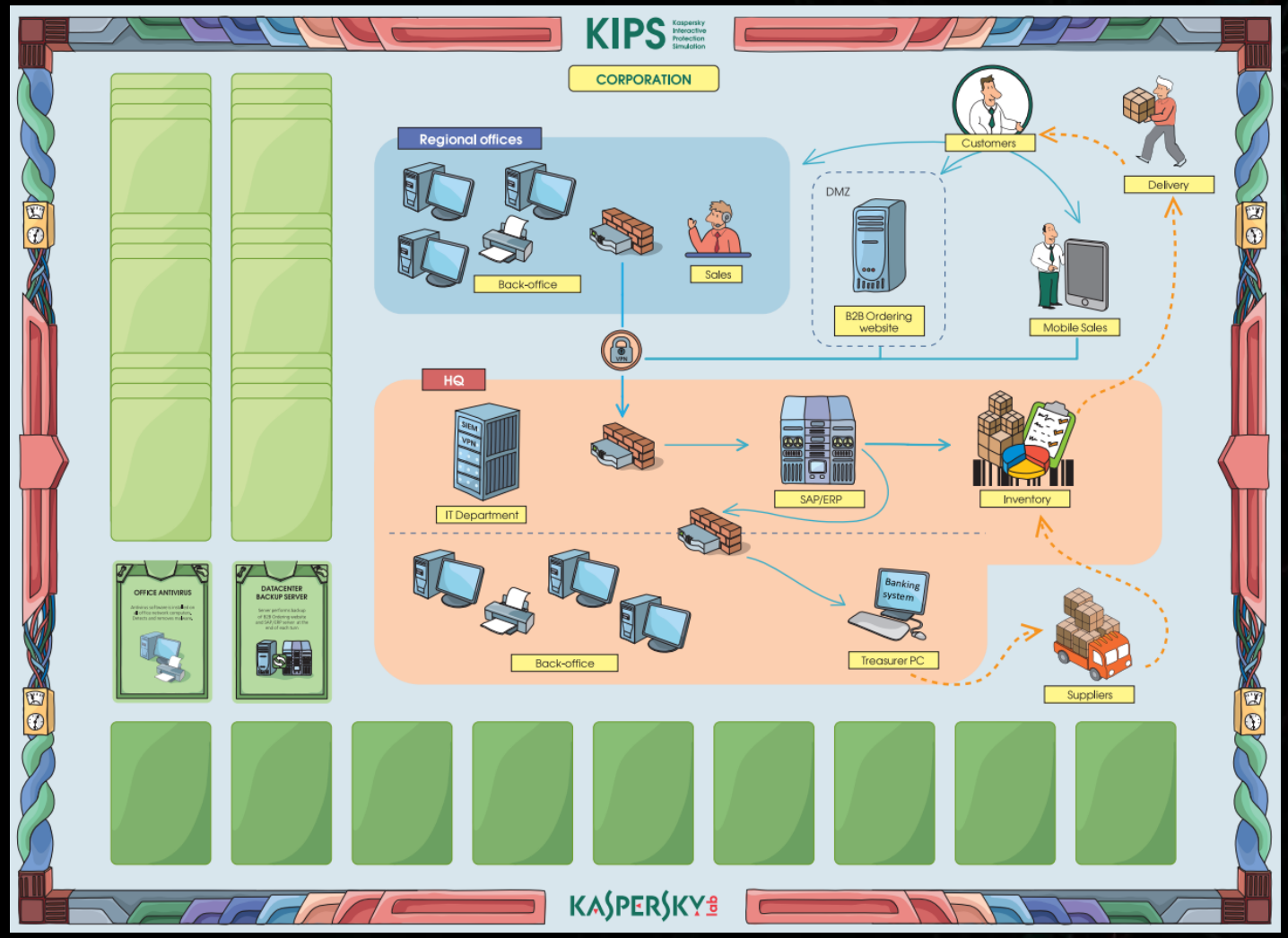
IT & BUSINESS MANAGERS

Focused on business efficiency, automation, new technologies

Mutual understanding and daily attention to cyberthreats between these 3 are crucial to successful cybersecurity in the modern business

KASPERSKY lab

KASPERSKY INTERACTIVE PROTECTION SIMULATION



Game Board

Web Console

Action Cards

KASPERSKY lab

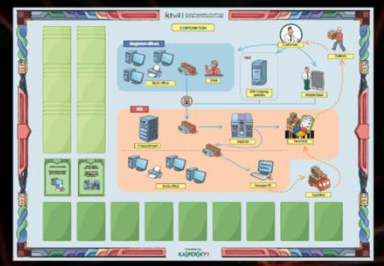
KASPERSKY INTERACTIVE PROTECTION SIMULATION

- Senior managers

For IT, Business and Security – strategy simulation
for cybersecurity decision-makers.

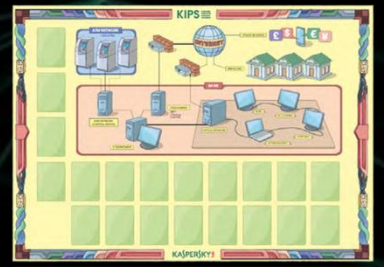
- Fun, engaging and fast (2 hours)
- Team-work builds cross-divisional co-operation
- Competition fosters initiative & analysis skills
- Gameplay develops an understanding of cybersecurity measures and strategy
- Teams compete at running a simulated enterprise and earning money

Corporate



Industrial

Financial



Government

KIPS Kaspersky Interactive Protection Simulation

KASPERSKY lab

Training process overview

Game rules and housekeeping explained

Trainer tells about the game and its rules, trainees listen and follow slides on a big screen.

20 minutes

KIPS is played by teams

Players read news and decide on actions by choosing cards according to their strategy and budget and time limitations.

After each turn a rating is updated.

Trainer facilitates, encourages and controls timing.

40 - 50 minutes

Ideal scenario unveiled and lessons learned

Trainer tells about threats met by players, unveils the ideal scenario and draw participants to conclusions and practical takeaways.

20 - 30 minutes

Results announced – congratulations to winners!

Participants can be invited to share results and photos on social media.

10 - 20 minutes

Overall 1,5 – 2 hours

KASPERSKY lab

VYZKOUŠEJTE TO S NÁMI....

ComputerWeekly

”The Kaspersky Interactive Protection Simulation was a real eyeopener and should be made mandatory for all security professionals.”

www.computerweekly.com/feature/Interactive-cyber-attack-a-dangerous-game

KASPERSKY lab

kaspersky

Děkuji Vám !